Rada
Evropské unie

Brusel 14. září 2017
(OR. en)

**Interinstitucionální spis:**
**2017/0225 (COD)**

**12183/17**
**ADD 2**

**CYBER 127**
**TELECOM 207**
**ENFOPOL 410**
**CODEC 1397**
**JAI 785**
**MI 627**
**IA 139**

**PRŮVODNÍ POZNÁMKA**

| | |
|---|---|
| Odesílatel: | Jordi AYET PUIGARNAU, ředitel,<br>za generálního tajemníka Evropské komise |
| Příjemce: | Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie |
| Č. dok. Komise: | SWD(2017) 501 final |
| Předmět: | PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE SOUHRN POSOUZENÍ DOPADŮ Průvodní dokument k návrhu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“) |

Delegace naleznou v příloze dokument SWD(2017) 501 final.

Příloha: SWD(2017) 501 final

EVROPSKÁ
KOMISE

V Bruselu dne 13.9.2017
SWD(2017) 501 final

**PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE**

**SOUHRN POSOUZENÍ DOPADŮ**

***Průvodní dokument k***

**návrhu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY**

**o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)**

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

## A. POTŘEBA OPATŘENÍ

### Jaký problém se řeší a proč jde o problém?

Digitální technologie a internet jsou páteří společnosti a hospodářství EU. Klíčová hospodářská odvětví, jako je doprava, energetika, zdravotnictví nebo finančnictví, jsou stále více závislé na sítích a informačních systémech. Internet věcí spojuje předměty a osoby prostřednictvím komunikačních sítí. Tato nová realita vytváří nebývalé příležitosti, avšak vede také k větší zranitelnosti. Takřka neustále dochází ke kybernetickým incidentům. Jejich komplexnost, četnost a dopad – od problémů s přístupem k základním službám až po ovlivňování demokratických procesů – se bude nadále zvyšovat.

V této souvislosti byly zjištěny následující problémy, jež spolu vzájemně souvisejí:

- roztříštěnost politik a přístupů ke kybernetické bezpečnosti v různých členských státech
- rozptýlené zdroje a roztříštěnost přístupů ke kybernetické bezpečnosti napříč orgány, institucemi a jinými subjekty EU
- nedostatečná informovanost občanů a podniků o kybernetických hrozbách a nedostatek informací o kybernetickobezpečnostních vlastnostech produktů a služeb IKT, které si pořizují, ve spojení se stále větším počtem nově vznikajících vnitrostátních a odvětvových systémů certifikace.

Tyto problémy mají dopad na celkovou kybernetickou odolnost Evropské unie a na účinné fungování vnitřního trhu.

### Čeho by mělo být dosaženo?

Specifické cíle této iniciativy jsou tyto:

1. zvýšit schopnosti a připravenost členských států a podniků, zejména pokud jde o kritické infrastruktury;
2. zlepšit spolupráci a koordinaci napříč členskými státy a orgány, agenturami a institucemi EU;
3. zvýšit úroveň schopností EU doplňovat opatření členských států, zejména v případě přeshraničních kybernetických krizí;
4. zvýšit informovanost občanů a podniků o otázkách týkajících se kybernetické bezpečnosti;
5. zvýšit celkovou transparentnost záruky kybernetické bezpečnosti produktů a služeb IKT, aby se posílila důvěra v jednotný trh a digitální inovace;
6. zamezit roztříštěnosti systémů certifikace v EU a souvisejících bezpečnostních požadavků a hodnoticích kritérií napříč členskými státy a odvětvími.

### Jakou přidanou hodnotu budou mít opatření na úrovni EU?

Vzhledem k tomu, že digitalizace a propojenost hospodářství a společnosti má globální dopady, sahají příslušné problémy daleko za hranice jednoho členského státu. Proto je nutný

zásah na úrovni Unie. Za stávající situace a při pohledu na možné budoucí scénáře se zdá, že individuální opatření členských států a roztříštěný přístup ke kybernetické bezpečnosti, zejména vzhledem k jejímu silnému přeshraničnímu rozměru, nemohou vést ke zvýšení společné kybernetické odolnosti Unie.

## B. ŘEŠENÍ

**Prostřednictvím kterých možností lze cílů dosáhnout? Je některá možnost upřednostňována?**

Toto posouzení dopadů zkoumá specifický soubor možných opatření, která zahrnují přezkum činnosti Agentury Evropské unie pro bezpečnost sítí a informací (ENISA) a certifikaci bezpečnosti IKT.

### *Přezkum ENISA*

**Možnost 0** – **základní scénář** – tato možnost zachovává současný stav. Mandát agentury ENISA by byl prodloužen a cíle a úkoly agentury by zůstaly v zásadě nezměněné, pouze by se zohlednily úkoly svěřené agentuře ENISA následně přijatými právními předpisy EU (např. směrnicí o bezpečnosti sítí a informací).

**Možnost 1** – **ukončení mandátu ENISA** (ukončení činnosti ENISA). Tato možnost by vedla k ukončení činnosti agentury ENISA na konci jejího mandátu (červen 2020) a případně k přerozdělení pravomocí a činností na úrovni EU a /nebo na úrovni členských států.

**Možnost 2** – **„reforma ENISA“**. Tato možnost politiky by vycházela ze současného mandátu agentury ENISA s výhledem na přijetí selektivních změn zohledňujících vývoj v oblasti kybernetické bezpečnosti. Agentura by získala trvalý mandát, jehož základem by byly tyto prvky: podpora tvorby a provádění politik EU; budování kapacit; znalosti a informace; úkoly související s trhem; výzkum a inovace; a operativní spolupráce a řešení krizí.

**Možnost 3** – **agentura EU pro kybernetickou bezpečnost s plnými operačními schopnostmi**. Tato možnost znamená reformu agentury ENISA prostřednictvím spojení tří hlavních funkcí: 1. politická/poradní funkce; 2. středisko informací a odborných znalostí; a 3. skupina pro reakci na počítačové hrozby (CERT). Tato možnost by do značné míry znamenala stejnou změnu rozsahu mandátu jako možnost 2. Byly by však přidány další úkoly v oblasti reakce na incidenty a řízení krizí, takže agentura by pokrývala celý životní cyklus kybernetické bezpečnosti a měla by na starosti prevenci a odhalování kybernetických incidentů i reakci na ně.

### *Certifikace*

**Možnost 0 – základní scénář – nečinnost**. V tomto případě by Komise zachovala současný stav a nepodnikala by žádné politické ani legislativní kroky.

**Možnost 1** – **nelegislativní („měkká“) opatření**. V rámci této možnosti by Komise použila měkké nástroje (jako jsou např. interpretační sdělení nebo podpora celoevropských samoregulačních iniciativ a aktivit v oblasti normalizace) s cílem zlepšit transparentnost a snížit roztříštěnost.

**<u>Možnost 2</u> – legislativní akt EU, kterým by se rozšířila dohoda SOG-IS na všechny členské státy**. V rámci této možnosti by Komise navrhla legislativní akt, kterým by se rozšířilo členství na všechny členské státy.

**<u>Možnost 3</u> – obecný rámec EU pro certifikaci bezpečnosti IKT**. Tato možnost znamená vytvoření evropského rámce certifikace bezpečnosti IKT (včetně skupiny odborníků složené ze zástupců vnitrostátních orgánů), jenž by v co nejvyšší možné míře vycházel ze stávajících systémů certifikace bezpečnosti IKT. Takový rámec by v zásadě umožnil vytvoření certifikačních systémů EU, které by byly uznávány napříč členskými státy.

Upřednostňovanou možností je kombinace možnosti 2 pro ENISA a možnosti 3 pro certifikaci.

**Kdo jsou zúčastněné strany? Kdo podporuje kterou možnost?**

Převážná většina zúčastněných stran ze všech kategorií (členské státy, průmysl, orgány EU, výzkumná obec), které se zúčastnily konzultací, očividně vítá upřednostňovanou možnost, jelikož tyto strany podporují posílení agentury ENISA a vytvoření evropského rámce certifikace bezpečnosti IKT.

Panuje zejména shoda ohledně nutnosti mít (alespoň) dobře fungující agenturu EU s trvalým mandátem, která bude mít odpovídající zdroje a mandát k tomu, aby čelila současným a budoucím kybernetickobezpečnostním výzvám. Mezi zúčastněnými stranami rovněž panuje široká shoda ohledně vytvoření dobrovolného evropského rámce, který bude možné přizpůsobit aktuálním potřebám.

Pokud jde o zástupce průmyslu, zvolené řešení pro certifikaci podporují podniky, na které se již vztahují požadavky certifikace a pro něž by byl celoevropský mechanismus vzájemného uznávání certifikátů přínosem. Podporují ho rovněž malé a střední podniky, které nejvíce trpí tím, že musí, nebo by musely absolvovat různé certifikační postupy v různých členských státech. Některé členské státy, zejména ty, jež mají k dispozici méně zdrojů, a někteří zástupci podniků a orgánů EU se vyjádřili kladně také k možnosti 3 pro ENISA.

## C. DOPADY UPŘEDNOSTŇOVANÉ MOŽNOSTI

**Jaké jsou výhody upřednostňované možnosti (je-li nějaká doporučena, jinak uveďte výhody hlavních možností)?**

Na základě upřednostňované možnosti by EU měla agenturu zaměřenou na poskytování podpory členským státům, orgánům EU a podnikům v oblastech, kde by mohla přinést největší přidanou hodnotu. Mezi tyto oblasti patří: podpora provádění směrnice o bezpečnosti sítí a informací; tvorba a provádění politiky; informace, znalosti a informovanost; výzkum; operativní spolupráce a řešení krizí; trh. Agentura ENISA by zejména podporovala politiku EU v oblasti certifikace bezpečnosti IKT tím, že by zajišťovala správu a technickou údržbu evropského rámce certifikace bezpečnosti IKT. Tímto rámcem bude zaveden soubor opatření pro správu certifikace bezpečnosti IKT v EU, což podpoří vzájemné uznávání certifikátů vydaných v různých členských státech. Řešení spočívající v kombinaci těchto možností je považováno za nejefektivnější způsob, jímž může EU dosáhnout stanovených cílů, a sice: zvýšení schopností v oblasti kybernetické bezpečnosti; připravenosti: spolupráce;

informovanosti; transparentnosti, a zamezení roztříštěnosti trhu. Tato možnost také nejvíce odpovídá politickým prioritám zakotveným ve strategii kybernetické bezpečnosti a souvisejících politikách (např. směrnici o bezpečnosti sítí a informací) a ve strategii pro jednotný digitální trh. Kromě toho by tato možnost vedla k dosažení cílů prostřednictvím přiměřeného využití zdrojů.

**Jaké jsou náklady na upřednostňovanou možnost (je-li nějaká doporučena, jinak uveďte náklady na hlavní možnosti)?**

Navzdory nově svěřeným úkolům zůstane „reformovaná ENISA“ agilní organizací. Potřebný finanční příspěvek z rozpočtu EU by byl vyšší než v současnosti, ale stále mnohem nižší než u ostatních agentur, které rovněž působí v kritických oblastech.

Vytvoření evropského rámce certifikace bezpečnosti IKT by neznamenalo další přímé náklady pro podniky (včetně malých a středních podniků). Naopak by přineslo značné úspory těm firmám, které již certifikují své produkty, nebo jsou ochotny absolvovat certifikaci bezpečnosti, a mělo by příznivé dopady na jejich konkurenceschopnost v celosvětovém měřítku. Na druhou stranu by znamenalo určité rozpočtové závazky, aby byla zajištěna správa rámce, kterou by, pokud jde o technické a administrativní úkoly, zajišťovala zejména „reformovaná ENISA“.

**Očekávají se významné dopady na vnitrostátní rozpočty a správní orgány?**

Ne. Náklady spojené s posílením agentury ENISA by měly být převážně hrazeny z rozpočtu EU, přičemž členské státy budou mít možnost poskytovat agentuře dobrovolné finanční příspěvky. Pokud jde o certifikaci, hlavní dopad na vnitrostátní rozpočty a správy bude mít vytvoření certifikačního orgánu.

**Očekávají se jiné významné dopady?**

Ne.

**Proporcionalita?**

Upřednostňovaná možnost obnáší vyvážená opatření považovaná za nezbytná k dosažení daných cílů, aniž by znamenala nepřiměřenou zátěž pro příslušné zúčastněné strany. Proto se má za to, že je tato iniciativa v souladu se zásadou proporcionality

## D. NÁVAZNÁ OPATŘENÍ

**Kdy bude tato politika přezkoumána?**

Navrhuje se, aby se první hodnocení uskutečnilo pět let po vstupu příslušného právního nástroje v platnost. Komise následně zprávu o hodnocení předloží Evropskému parlamentu a Radě, případně spolu s návrhem na přezkum. Další hodnocení se budou muset provádět každých pět let.